Junos Pulse 2.1 Release Notes
Junos Pulse Build# 14305
Secure Access Build# 7.1R5
JWOS Build# 6.2R1.4
Contents

Junos Pulse 2.1 Release Notes .......................................................................................................................... 1
Junos Pulse 2.1 – New Features .......................................................................................................................... 3
  Application Acceleration ................................................................................................................................. 3
  Junos Pulse and iPass Open Mobile – Advanced Connectivity ................................................................. 3
  Pulse Launcher ............................................................................................................................................. 3
  Junos Pulse 2.1 Supports JWOS 6.2 ............................................................................................................. 3
Installing and Deploying Junos Pulse 2.1 ...................................................................................................... 3
Interoperability and Supported Platforms ..................................................................................................... 4
Junos Pulse Client Availability ....................................................................................................................... 4
Known Issues Fixed in Junos Pulse 2.1 .......................................................................................................... 4
Known Issues and Limitations .......................................................................................................................... 4
  Junos Pulse 2.1 ........................................................................................................................................... 4
  Installation and Configuration ....................................................................................................................... 5
  Unified Access Control ................................................................................................................................. 6
  Secure Access ............................................................................................................................................ 6
  Endpoint Security ....................................................................................................................................... 7
  SRX ............................................................................................................................................................. 7
  802.1x ....................................................................................................................................................... 8
  Application Acceleration ............................................................................................................................ 8
Communicating Issues .................................................................................................................................... 8

For information about supported minimum requirements for Network and Security Manager (NSM), please refer to the Juniper Networks Network and Security Manager Installation Guide.
Junos Pulse 2.1 – New Features

Application Acceleration

Junos Pulse 2.1 (for Microsoft Windows) introduces Application Acceleration for SSL and MAPI as a Pulse service. Pulse 2.1 introduces a disk-based compression service with NSC (Network Sequence Caching) that works in tandem with the existing memory-based compression (LZ). Junos Pulse 2.1 users will experience enhanced performance over WAN connections for MAPI, SSL, HTTP and CIFS sessions from their desktops and laptops.

Application Acceleration support is not available for smart phones.

<table>
<thead>
<tr>
<th>Compatible with:</th>
</tr>
</thead>
<tbody>
<tr>
<td>JWOS 6.2</td>
</tr>
</tbody>
</table>

Junos Pulse and iPass Open Mobile – Advanced Connectivity

Junos Pulse Release 2.1 supports select third-party software integration. iPass Open Mobile Platform provides reliable, secure, and high-performance deployment of iPass enterprise mobility services. Together Pulse and iPass expand secure access options for Windows XP, Windows Vista, and Windows 7 endpoints. Third-party application integration is supported by Junos Pulse Secure Access Service. iPass Enterprise Mobility Services provide authorized connectivity to public networks for Pulse users. Mobile users can connect to any Wi-Fi, Mobile Broadband, or dial-up network from the iPass Networks list. Once the Internet connection is established, Junos Pulse provides a secure connection to the enterprise resources. iPass Enterprise Mobility Services provide authorized secure access to networks in restaurants, airports and in-flight Wi-Fi hot spots.

Pulse Launcher

Pulse Launcher is a standalone 32-bit executable that runs on any supported Windows platform. It provides a command-line interface for users to connect and disconnect to either Pulse Access Control Service or Pulse Secure Access Service gateways.

Junos Pulse 2.1 Supports JWOS 6.2

Junos Pulse 2.1 interoperates with MAG Series Junos Pulse Gateways running JWOS 6.2 only. Pulse 2.1 does not support JWOS 6.1 or JWOS 6.0.

Installing and Deploying Junos Pulse 2.1

There are several ways to deploy Junos Pulse to endpoints:

- Create a custom configuration on the Pulse Secure Access server or Pulse Application Acceleration server, and then direct users to navigate to the access device for an automatic download through a role. This is the simplest way to deploy Pulse!
- Create a custom configuration, download an installer package, and distribute to users through a System Management Server (SMS).
- Download the default installer from the Maintenance > System > Installers page on a Pulse Secure Access server and distribute to users.

With the default installer, all components and connections needed for connecting to an access device are included in the client.
For custom configurations, you create component sets and connection sets on the SA Series device, and then download an installer package. See the *Junos Pulse Administration Guide* for complete instructions.

**Interoperability and Supported Platforms**

- Please refer to the *Pulse Supported Platforms* document for supported versions of Screen OS, JUNOS, browsers, and operating systems in this release: [http://www.juniper.net/support/products/pulse](http://www.juniper.net/support/products/pulse)

**Junos Pulse Client Availability**

- Pulse packages are available for download from [http://www.juniper.net/support/products](http://www.juniper.net/support/products)
- Log in with your Juniper support account to download any Pulse packages.

**Known Issues Fixed in Junos Pulse 2.1**

The following issues are fixed in this release:

- In 802.1q VLAN environments that support tagging of out-of-band data, out-of-band packets may receive an in-band tag. (PR 687730)
- Junos Pulse prompts for a secondary username even when the name is defined in the secondary authentication page on the Secure Access server. The Secure Access server must have version 7.1R5 or later to support this fix. (PR 486571)

**Known Issues and Limitations**

The following known issues are outstanding in this release:

**Junos Pulse 2.1**

- When using a Smartcard, the user is prompted by either the Smartcard provider or Microsoft Base Smartcard Crypto Provider CSP for the PIN/Password. This prompt is not managed by Pulse and may remain displayed after a Pulse connection is disconnected or the Pulse process has exited. (PR 549408)
- When Custom SSL Cipher Selection is chosen on the Pulse Access Control server and AES alone is selected, Pulse connections from XP clients will not work. This is a limitation due to the cryptography available from the Windows XP operating system. (PR 516592,555704)
- Pulse UI does not display correctly in High Contrast graphics settings. (PR 490249)
- The F1 key does not display the Table of contents help window. (PR 484222)
- Disabling "Allow user to override connection policy" results in a user not being able to connect if the connection policy indicates a connection should not be made. (PR 498065)
- Disabling Junos Pulse Split Tunneling on a Secure Access device may impact the ability for Pulse to evaluate Location Policies associated with the physical interface on the endpoint. (PR 506100)
- When using a packet capture / monitor tool like Wireshark or NetMon (on XP), certain IP packets sent may appear to be sent twice. This is most often observed when the network capture mechanism enables Promiscuous Mode on the network adapter. (PR 514609)
- Trailing white space is not pruned when entering user credentials within Pulse. (PR 513433)
- If Junos Pulse is uninstalling while connected to a Pulse Secure Access server or Pulse Access Control server, the Pulse user session on the Pulse Secure Access server or Pulse Access Control server may not be deleted immediately. The session will be removed from the device when the user session's Heart Beat interval on the Pulse Access Control server or Idle Timeout on the Pulse Secure Access server expires. (PR 488572)
- If the Pulse UI displays "Connect Requested" connection status for an extended period of time and no progress is shown in establishing the connection, clicking disconnect followed by connect should allow the connection to proceed. (PR 514890)
- The Pulse UI may not display correctly on screen resolutions of 800 x 600 or less. (PR 524205)
- Pulse does not support certificate based authentication with certificates created or imported with "enable strong private key protection" feature. (PR 518468)
- Pulse may take 2-3 minutes to reconnect to an active node after a manual vip-failover occurs. (PR 518027)

Installation and Configuration

- The Junos Pulse configuration file cannot be downloaded from a Pulse Secure Access server or Pulse Access control server when used with Internet Explorer’s default security settings. The workaround is to add the Pulse Secure Access server or Pulse Access Control server IP address to the trusted site list under Tools->Internet Options->Security->Trusted Sites. (PR 581648)
- Once Junos Pulse 2.0 is installed, it is not advisable to use the standalone Pulse 1.0 installer. This may result in failures to uninstall any Junos Pulse 1.0 components. (PR 575731)
- When upgrading to Junos Pulse 2.0 using the MSI installer package, it may take several minutes to remove the previous version of Junos Pulse. During that time, the system may appear to be hung. This issue is caused by the Windows Installer doing verbose logging. The issue is documented and discussed in Microsoft KB article http://support.microsoft.com/kb/971133. (PR 559861)
- If the RSA Soft Token application (RSA 4.1.0.458) is installed after the Junos Pulse 2.0 is installed, you must reboot the system in order for Junos Pulse to detect the presence of the soft token application. (PR 543379)
- Canceling the Junos Pulse client installation is currently not supported. (PR 492565)
- Pulse deployed via dynamic deployment from a Pulse Secure Access server or Pulse Access Control server cannot be upgraded using the full installer package. (PR 513007)
- Some users may experience extended install times for Juniper's network driver component. (PR 94736)
- Some versions of Windows XP contain a known issue that causes extended install times for Pulse. Please refer to MS Incident KB949900 for a patch that should resolve the issue (http://support.microsoft.com/default.aspx/kb/949900). (PR 519639)
- Pulse installation on Vista x64 may not pre-install Juniper Networks Virtual Adapter instances. The first time a Pulse connection is established that requires a Juniper Networks Virtual Adapter instance the adapter will be installed resulting in a slight delay during the first connection. (PR 521929)
- If the user receives the error message “error provisioning access method connection” when attempting to establish a connection, it is possible that a third party USB device is interfering with the Juniper Networks Virtual Adapter. (PR 527406)
- When attempting to establish connections, Pulse may prompt you multiple times to upgrade 'missing components'. (PR 529409)
- Configuration changes to Pulse Secure Access server or Pulse Access Control servers that result in deploying new Firewall, 802.1x, or WX connections may require end users to re-login to the device via the web browser. (PR 523193)
- The Pulse Secure Access server or Pulse Access Control server administrator must associate a connection set with Pulse enabled user roles in order for Pulse to be properly deployed to endpoints. Pulse will not be installed or upgraded if the Pulse role references an empty connection set. (PR 525667)
- Pulse pre-configured installers can not re-bind the endpoint when it is already bound to a server. (PR 524357)
- If Junos Pulse and Kaspersky AntiVirus are installed and you attempt to uninstall Pulse, the popup message "Error!Can't initialize plug-ins directory please try again later..." may be displayed. If this occurs, try uninstalling Pulse again. (PR 528694)
Unified Access Control

- Junos Pulse 1.0 should not be installed with the Odyssey Access Client 5.3. (PR 545524)
- After changing an IPSec Policy on a Pulse Access Control server to ‘force VA’, Pulse may not configure the IPSec Virtual Adapter for the active user. (PR 492887)
- If you are using UAC IPSec Enforcement using Junos Pulse, applications might experience a slight delay in being able to establish network connections. (PR 491848)
- When you configure Junos Pulse to make 802.1x based connections, a reboot may be required on Windows XP the next time Junos Pulse is upgraded. (PR 492843)
- Establishing a connection to a Pulse Access Control server via the Pulse client is not supported when there is an existing active connection to the Pulse Access Control server with Odyssey Access Client. (PR 509095)
- NAP Host Checker Policies will not work with Pulse if Odyssey Access Client is installed and also evaluating NAP Host Checker Policies. (PR 512884)
- Certain client firewalls may make the Pulse connection on the Pulse Access Control server appear as if it is located behind a NAT device when it is not. (PR 519630)
- If connected to a Pulse Secure Access server and a Pulse Access Control server, then disconnect from the Pulse Secure Access server, other Pulse clients may receive the error "Too many connections from the same endpoint" error while attempting to connect to the Pulse Access Control server. (PR 528650)
- When both Pulse and the Odyssey Access Client are installed on the same machine, Juniper recommends that only one client be used when establishing connections to the same Pulse Access Control server. (PR 526333)
- While Pulse is connected to a Pulse Access Control server and the user initiates a connection to a Firewall, the Pulse Access Control server connection may get disconnected. (PR 524075)
- When Pulse has connections to both a Pulse Secure Access server and Pulse Access Control server and the user disconnects from the Pulse Access Control server, the Active Users page may shows that the user session is still active. (PR 523750).

Secure Access

- During XML import and export, the role option “Enable 3rd party integration” is not present in the resultant XML file. Workaround is to manually enable/disable this option on the role. (PR 567600)
- When the Junos Pulse default connection is to a Pulse Secure Access server and the user logs off the Pulse Secure Access server from a browser, the default connection will remain connected. (PR 516180)
- When using a USB EVDO modem to connect to a Pulse Secure Access server, Junos Pulse may not provide network access after connecting successfully. (PR 583893)
- Junos Pulse connections may toggle between connecting and connected when Kaspersky Internet Security is active on the endpoint and Route Monitoring is enabled at the role-level. To workaround this issue, disable Route Monitoring on the Pulse Secure Access server. (PR 562789)
- To connect to a Pulse Secure Access server with Junos Pulse and Kaspersky anti-virus installed, split tunneling must be enabled. (PR 557069)
- Multiple simultaneously connected Pulse Secure Access server connections are not supported in Junos Pulse.
- Changes made to Junos Pulse configuration on Pulse Secure Access servers and Pulse Access Control servers are not showing up in the Admin Access Logs. (PR 475507)
- It is currently not possible to provide Junos Pulse access for the delegated admin role on Pulse Secure Access servers or Pulse Access Control servers. (PR 477822)
- When running Junos Pulse within Secure Virtual Workspace, the Pulse user interface will not launch correctly if it is also running on the base desktop. (PR 483290)
- When using the Firefox browser to deploy Pulse from a Pulse Secure Access server or Pulse Access Control server, please be sure that “Enable the next generation Java Plugin” is enabled in the Java console. (PR 498586)
Please be sure to install 32-bit version of Java runtime on 64-bit windows versions when deploying pulse via the Firefox browser. (PR 502486)

SAML OAAM authentication is not supported with the Pulse client. (PR 505578)

XML Export of the Pulse Configuration from a Pulse Secure Access server or Pulse Access Control server is exporting connection type as 802.1x for WX connection in Junos Pulse connection sets. (PR 513816)

Junos Pulse may not be able to connect correctly to a Pulse Secure Access server configured for secondary authentication when certificate authentication and local authentication are configured as primary/secondary authentication servers. (PR 489989)

When client proxy or server proxy is configured, if a user clicks on Sign out from the browser while Pulse NC is connected or if the Pulse NC user is timed out, Pulse may go into an infinite reconnect loop. This is because the proxy PAC file set by NC AM is not reverted in this situation, thus blocking Pulse from reconnecting. To come out of this situation, the end user must click disconnect on the Pulse UI and try to connect again. (PR 521906)

**Endpoint Security**

- Shavlik Remediation may fail on endpoints running Kaspersky Antivirus 6.0 for Windows workstations. The patch remediation may succeed if the Kaspersky Antivirus software is turned off. (PR 573973)

- When using Patch Remediation, the patch installation count may exceed the missing patch count. This may occur when the same patch is attempted to be installed twice. The result will be a failure during the second attempt, which should be ignored. Two known patches that can exhibit this issue, WindowsXP-KB954459.exe on Windows XP and msxml6-KB954459.exe. (PR 561392)

- During patch remediation after auto remediation complete, the user may be prompted to reboot the system. If the user attempts to connect prior to rebooting, the connection may pass the compliance check. An example of such a patch is the WindowsXP-KB953155.exe. (PR 575714)

- When a Shavlik policy is configured and a browser is used to login and launch Junos Pulse, high CPU utilization may be observed. To avoid this issue, the user should login directly using Junos Pulse. (PR 565692)

- During patch installation, some anti-malware solutions may report a risk warning on stdeploy.exe. To avoid the warning, add Hostcheckpluginhost.exe to the anti-malware exceptions list; otherwise user’s can safely ignore the warning to continue. (PR 573970)

- When Enhanced Endpoint Security (EES) is enabled and the user installs Junos Pulse via a browser, the upgrade prompt may be shown immediately after connecting to the Junos Secure Access server. (PR 574762)

- When using Shavlik Remediation with proxy credentials, Junos Pulse may stay in the connecting state. To workaround this issue, wait a few seconds before entering the proxy credentials (PR 523146).

- In Junos Pulse, the Shavlik remediation dialog prompt may flash when transitioning from the certificate to credentials dialog. (PR 544665)

- For testing Patch Remediation feature for restricted user account, the machine should be rebooted after Pulse installation in admin account. If user switches to restricted user without rebooting then Patch Installation Progress dialog does not appear. (PR 560962)

**SRX**

- Installing Junos Pulse 1.0 after installing JAM 1.0 is not supported.

- When using SecurID to authenticate, Junos Pulse 2.0 does not request a new passcode when reconnecting. (PR 570033)

- When using SecurID to authenticate, Junos Pulse 2.0 requests user to enter the password instead of token information. (PR 570037)

- When using Dynamic-VPN with the SRX-240 configured to use xauth authentication through the radius server, the IPSec tunnel may not get established when the virtual adapter is created.(PR 576246)

- Save credentials in the Junos Pulse credential dialog is not working correctly for SRX connections. (PR 490482)
• For firewall connections, the "Forget saved settings" option may not clear all saved data. (PR 492880)

802.1x

• Junos Pulse doesn't show authentication failure when using 802.1x connections and an expired client certificate is used. (PR 487727)
• When using Junos Pulse 802.1x connections on Windows XP with Odyssey Access Client installed, you will have to check the check box, "use windows to configure my wireless network settings", manually after you uncheck "use Odyssey to operate this adapter" in Odyssey Access Client. (PR 504701)
• Pre-configuration of 802.1x settings is required in order for the 802.1x feature to work correctly if users cannot log-in to the Pulse Access Control server via the web browser to dynamically deploy the configuration. (PR 526341)

Application Acceleration

• The Junos Pulse Application Acceleration component may cause disruptions with some types of network connections on systems with multiple network interfaces that are connected simultaneously. (PR 504692)
• Deploying the Junos Pulse WAN Application Acceleration package via Host Checker is not supported when logging in via the Junos Pulse client. This is only applicable to browser based initial deployments. (PR 504952)
• Firewalls like Kaspersky software are known to block Pulse Application Acceleration control packets. UDP port 3578 must be provisioned to open ports at the endpoint. (PR 505817)
• If Junos Pulse software requires the Application Acceleration capability to be deployed from a Pulse Secure Access server, ‘All components’ should be selected at the Pulse Secure Access server. (PR 505944)
• Pulse may disrupt Internet Connection Sharing via Windows Virtual Wi-Fi on Windows 7 Endpoints when Application Acceleration is installed. (PR 507628)
• When you try to collect "LogsAndDiagnostics.zip" from Pulse, Save logs in Windows Vista and Windows7 "User Account Control" window pops up. The solution is to click "Yes/Continue" in "User Account Control" window to collect Logs successfully. (PR 666394)
• Junos Pulse Application Acceleration Service does not apply ACLs on diskcache folder (i.e.JWACDiskCache), if the file system does not support security attributes. (Like FAT32 file system which does not support ACL’s). (PR 678387)

Communicating Issues

To open a case or to obtain support information, please visit the Juniper Networks Support Site: http://www.juniper.net/support.